



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/697,929	10/31/2003	Rajesh K. Shenoy	200309942-1	8942
22879	7590	09/20/2007	EXAMINER	
HEWLETT PACKARD COMPANY P O BOX 272400, 3404 E. HARMONY ROAD INTELLECTUAL PROPERTY ADMINISTRATION FORT COLLINS, CO 80527-2400			COLIN, CARL G	
			ART UNIT	PAPER NUMBER
			2136	
			MAIL DATE	DELIVERY MODE
			09/20/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/697,929

Applicant(s)

SHENOY ET AL.

Examiner

Carl Colin

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 05 July 2007.
- 2a) This action is **FINAL**. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-24 is/are pending in the application.
 - 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-24 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some * c) None of:
 - 1. Certified copies of the priority documents have been received.
 - 2. Certified copies of the priority documents have been received in Application No. _____.
 - 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) Notice of References Cited (PTO-892)
- 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) Notice of Informal Patent Application
- 6) Other: _____

DETAILED ACTION

Response to Arguments

1. In communications filed on 7/5/2007, applicant amends claims 1, 10, 11, 13, 14, and 24. Claims 1-24 are presented for examination.

2. Applicant's arguments filed on 7/5/2007, pages 6-9, have been fully considered but they are not persuasive. Applicant argues that Gormish does not disclose a single multi-function peripheral as amended but rather requires three separate devices referring to col. 7, lines 11-29. However, Examiner would like to direct applicant to consider other embodiments disclosing a multifunctional device for scanning, storage, input/output interface, encryption, and decryption (see for instance, device of fig. 7 with detailed description and device 106 (column 4, lines 57-61; column 5, lines 54-64). Regarding providing secure access to a document, Gormish discloses enabling a user to enter key for causing access to enable the decryption of the encrypted document that meets the recitation of enabling access to the contents of the encrypted document utilizing a key by an authorized user (see column 10, line 65 through column 11, line 8). Applicant argues "Smith does not disclose any multifunction peripheral able to provide secure access to a document stored on the peripheral"; however, Gormish discloses this limitation as discussed above. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Art Unit: 2136

Therefore, applicant's arguments with respect to claim 1 are not persuasive as amended.

Arguments of the other claims are related to claim 1 and therefore they are not persuasive. Upon further consideration, it remains the Examiner's position that claims 1-24 are still rejected in view of the same prior art.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-6 and 10-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,692,048 to **Gormish et al** in view of US Patent Publication 2003/0005298 to **Smith et al**.

As per claim 1, Gormish et al substantially teaches a secure document access method comprising: *at a multifunctional peripheral* (see for instance, device of fig. 7 with detailed description and device 106 (column 4, lines 39-65; column 5, lines 54-64) *capturing contents of*

Art Unit: 2136

a document (see column 10, lines 29-38); *generating a key from a cryptographic engine* (see column 12, lines 22-25 and lines 34-36) (device 107 comprises controller for encryption (see column 38-45 and device 106 comprises encryption component for providing its own encryption process (see column 5, lines 54-58); *encrypting the contents of the document using said key by a multi-function peripheral* (see column 15, lines 40-45; column 5, lines 1-7 and lines 44-47; and column 10, line 66 through column 11, line 7); *storing said encrypted document* (see column 8, lines 18-20 and claim 20); *and enabling access to the contents of the encrypted document utilizing said key by the at least one authorized user* (see column 15, lines 45-47; column 10, line 65 through column 11, line 8). **Gormish et al** suggests using any digital encryption method and any key exchange methods and use of keys as known in the art (see column 6, lines 29-47; column 11, lines 6-7 and column 12, lines 57-59) but does not explicitly disclose encoded the key and communicated the encoded key. **Smith et al** in an analogous art teaches a method and apparatus for authenticating ownership of cryptographic keys comprising generated a key, the key is hashed and encoded into a bar code; then the encoding key is communicated to the receiver as the encoded key is applied to the transmitted document (see page 2, paragraphs 18-20 and figure 2) that meets the recitation of *communicating the encoded key to at least one authorized user*. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include the features of encoding as disclosed in **Smith et al** to encode the keys of **Gormish et al** as taught by **Smith et al** (see figure 2). One of ordinary skill in the art would have been motivated to do so because it would provide a secure means to communicate key information associated with the sender and the document (see paragraph 15) as

Art Unit: 2136

well as way to verify the sender of the document as suggested by **Smith et al** (see page 2, paragraphs 17-21).

As per claim 2, the combination of **Gormish et al** and **Smith et al** discloses wherein the encoded key is transmitted to the at least one authorized user in an electronic form (see **Smith et al**, page 2, paragraphs 16 and 20). Therefore, claim 2 is rejected on the same rationale as the rejection of claim 1 above.

As per claim 3, the combination of **Gormish et al** and **Smith et al** discloses the key is encoded into UPC symbol or bar code and may be imprinted on the document (see **Smith et al**, paragraphs 12, 16, and 19), it is apparent that UPC symbol or bar code represents black and white pattern which meets the recitation of wherein the encoded key is represented by a half-tone pattern as interpreted by Examiner. Therefore, claim 3 is rejected on the same rationale as the rejection of claim 1 above.

As per claim 4, the combination of **Gormish et al** and **Smith et al** discloses the key is encoded and imprinted on the document (see **Smith et al**, page 2, paragraph 16), which meets the recitation of wherein the encoded key is output via a printer. Therefore, claim 4 is rejected on the same rationale as the rejection of claim 1 above.

As per claim 5, the combination of **Gormish et al** and **Smith et al** discloses using cryptographic techniques to send the encoded key and **Smith et al** further describes secure

Art Unit: 2136

communications when the two parties use encryption techniques to communicate (see paragraphs 5, 6, and 16), which meets the recitation of wherein the encoded key is transferred to the at least one authorized user in a secure manner. Therefore, claim 5 is rejected on the same rationale as the rejection of claim 1 above.

As per claim 6, the combination of **Gormish et al** and **Smith et al** discloses wherein the cryptographic key is generated via a software process (see **Gormish et al**, column 12, lines 22-25 and lines 34-36).

As per claim 10, the combination of **Gormish et al** and **Smith et al** discloses enabling the authorized user to access the document at a second multi-function peripheral (see **Gormish et al**, column 5, lines 15-38 and figure 1).

As per claim 11, the combination of **Gormish et al** and **Smith et al** discloses wherein said accessing of the encrypted document comprises the steps of: decoding said encoded key (see **Smith et al**, paragraph 20); locating the encrypted document; retrieving the encrypted document (see **Gormish et al**, column 8, lines 35-39); decrypting the contents of the encrypted document (see **Gormish et al**, column 8, lines 45-50 and column 15, lines 45-51); and outputting contents of the document (see **Gormish et al**, column 8, lines 45-50 and column 15, lines 45-51). (See also column 5, lines 54-64 and column 15, lines 45-47 and column 10, line 65 through column 11, line 8 with respect to multi-function peripheral). Claim 11 is rejected on the same rationale as the rejection of claim 1 above.

As per claim 12, the combination of **Gormish et al** and **Smith et al** discloses wherein contents of the document are captured line by line using imaginary line as an example (see **Gormish et al**, column 16, lines 51 through column 17, line 5).

As per claim 13, **Gormish et al** substantially teaches a system for accessing a secure document comprising: a computing device coupled to a multifunction peripheral said peripheral including (see for instance, device of fig. 7 with detailed description and device 106 (column 4, lines 39-65 and column 5, lines 54-64) discloses each of the devices comprises scanner with *means for capturing contents of a document* (see column 10, lines 29-38; column 4, lines 57-60 and fig. 7); *means for generating a key from a cryptographic engine* (see column 12, lines 22-25 and lines 34-36) (device 107 comprises controller for encryption (see column 38-45 and device 106 comprises encryption component for providing its own encryption process (see column 5, lines 54-58); *means for encrypting the contents of the document using said key by a multi-function peripheral* (see column 15, lines 40-45; column 12, lines 19-21 and column 10, line 66 through column 11, line 7), the multi-function peripheral is described in column 4, lines 39-65; *means for storing said encrypted document* (see column 8, lines 18-20; fig. 7 (data storage), and claim 20); *and means for enabling access to the contents of the encrypted document utilizing said key by the at least one authorized user* (see column 15, lines 45-47 and column 10, line 65 through column 11, line 8). **Gormish et al** suggests using any digital encryption method and any key exchange methods and use of keys as known in the art (see column 6, lines 29-47; column 11, lines 6-7 and column 12, lines 57-59) but does not explicitly disclose encoded the key and

Art Unit: 2136

communicated the encoded key. **Smith et al** in an analogous art teaches a method and apparatus for authenticating ownership of cryptographic keys comprising generated a key, the key is hashed and encoded into a bar code; then the encoding key is communicated to the receiver as the encoded key is applied to the transmitted document (see page 2, paragraphs 18-20 and figure 2) that meets the recitation of *means for communicating the encoded key to at least one authorized user*. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include the features of encoding as disclosed in **Smith et al** to encode the keys of **Gormish et al** as taught by **Smith et al** (see figure 2). One of ordinary skill in the art would have been motivated to do so because it would provide a secure means to communicate key information associated with the sender and the document (see paragraph 15) as well as way to verify the sender of the document as suggested by **Smith et al** (see page 2, paragraphs 17-21).

As per claim 14, Gormish et al substantially teaches a multi-function peripheral comprising: (see for instance, device of fig. 7 with detailed description and device 106 (column 4, lines 39-65; column 5, lines 54-64) *a scanner for capturing contents of a document* (see column 10, lines 29-38; column 4, lines 57-60; and fig. 7); *a cryptographic engine for generating a cryptographic key* (see column 12, lines 22-25 and lines 34-36) (device 107 comprises controller for encryption (see column 38-45 and device 106 comprises encryption component for providing its own encryption process (see column 5, lines 54-58); *application programmed to encrypt the contents of the document* (see column 15, lines 40-45; column 12, lines 19-21 and column 10, line 66 through column 11, line 7), *a memory device for storing*

Art Unit: 2136

contents of the document (see column 8, lines 18-20; fig. 7 (data storage), and claim 20); *and a facsimile device for transmitting data* (see column 15, lines 45-47 and column 11, lines 6-8) *wherein said peripheral enables an authorized user to access said document at said peripheral using said encoded key* (see column 15, lines 45-47 and column 10, line 65 through column 11, line 8). **Gormish et al** suggests using any digital encryption method and any key exchange methods and use of keys as known in the art (see column 6, lines 29-47; column 11, lines 6-7 and column 12, lines 57-59) but does not explicitly disclose encoded the key. **Smith et al** in an analogous art teaches a method and apparatus for authenticating ownership of cryptographic keys comprising generated a key, the key is hashed and encoded into a bar code; then the encoding key is communicated to the receiver as the encoded key is applied to the transmitted document (see page 2, paragraphs 18-20 and figure 2) that meets the recitation of *at least one application specific integrated circuit (ASIC) programmed to encrypt contents of the document and to encode the cryptographic key* (see paragraph 18). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include the features of encoding as disclosed in **Smith et al** to encode the keys of **Gormish et al** as taught by **Smith et al** (see figure 2). One of ordinary skill in the art would have been motivated to do so because it would provide a secure means to communicate key information associated with the sender and the document (see paragraph 15) as well as way to verify the sender of the document as suggested by **Smith et al** (see page 2, paragraphs 17-21).

As per claim 15, the combination of **Gormish et al** and **Smith et al** discloses a digital sender unit for submitting the encoded key to a recipient in an electronic manner (see **Smith et**

Art Unit: 2136

al, paragraphs 10 and 13). Therefore, claim 15 is rejected on the same rationale as the rejection of claim 14 above.

As per claim 16, the combination of **Gormish et al** and **Smith et al** discloses two multi-function peripheral communicating over a network including network interface that meets the recitation of a network card (see **Gormish et al** figure 1 and 7) it is implicit that the devices disclosed by **Gormish et al** and **Smith et al** contain network card (see also **Smith et al**, paragraph 18).

As per claim 17, the combination of **Gormish et al** and **Smith et al** discloses wherein the network is a secure network (see **Gormish et al**, column 3, lines 50-67 and column 2, lines 66-67).

As per claim 18, the combination of **Gormish et al** and **Smith et al** discloses wherein said cryptographic engine is another application specific integrated circuit (ASIC) (see **Gormish et al**, column 12, lines 19-25). **Smith et al** discloses the invention may be implemented into small peripheral devices that implicitly contain ASIC chips (see paragraph 18).

As per claim 19, the combination of **Gormish et al** and **Smith et al** discloses wherein said cryptographic engine is a software process (see **Gormish et al**, column 12, lines 19-25).

Art Unit: 2136

As per claim 20, the combination of **Gormish et al** and **Smith et al** discloses wherein said at least one ASIC is programmed to decrypt the encrypted document (see **Gormish et al**, column 12, lines 19-25). **Smith et al** discloses the invention may be implemented into small peripheral devices that implicitly contain ASIC chips (see paragraph 18) wherein said at least one ASIC is programmed to decode the encoded key and to decrypt the encrypted document (see paragraphs 5 and 18). Claim 20 is rejected on the same rationale as the rejection of claim 14 above.

As per claim 21, the combination of **Gormish et al** and **Smith et al** discloses the key is encoded and imprinted on the document (see **Smith et al**, page 2, paragraph 16), which meets the recitation of a printer for outputting the key in the encoded form. Therefore, claim 21 is rejected on the same rationale as the rejection of claim 14 above.

As per claim 22, the combination of **Gormish et al** and **Smith et al** discloses wherein the at least one ASIC is programmed to generate the cryptographic key (see **Gormish et al**, column 12, lines 19-25 and 34-36). **Smith et al** discloses the invention may be implemented into small peripheral devices that implicitly contain ASIC chips (see paragraph 18).

As per claim 23, the combination of **Gormish et al** and **Smith et al** discloses the multi-function peripheral of claim 14, **Gormish et al** discloses a facsimile machine transmitting encoded information. **Smith et al** discloses wherein the facsimile machine transmits the key in the encoded form (see page 2, paragraphs 18-20 and figure 2) (see **Smith et al**, page 2, paragraph

Art Unit: 2136

4 suggesting fax communication). Therefore, claim 23 is rejected on the same rationale as the rejection of claim 14 above.

As per claim 24, Gormish et al substantially teaches machine readable medium comprising a computer program for causing a computer to: *create a document* (see column 10, lines 29-38); *submit the document to a peripheral having a cryptographic engine* (see column 12, lines 22-25 and column 15, lines 40-45); *and instruct the peripheral to encrypt contents of the document* (see column 15, lines 40-45; column 12, lines 19-21 and column 10, line 66 through column 11, line 7), *said instructions further causing the peripheral to* (see for instance, device of fig. 7 with detailed description and device 106 (column 4, lines 39-65; column 5, lines 54-64): *generate a key from the cryptographic engine* (see column 12, lines 22-25 and lines 34-36) (device 107 comprises controller for encryption (see column 38-45 and device 106 comprises encryption component for providing its own encryption process (see column 5, lines 54-58); *storing the encrypted document* (see column 8, lines 18-20; fig. 7 (data storage), and claim 20); *and transmit the key to at least one authorized user for accessing the encrypted document* (see column 15, lines 45-47 and column 8, lines 39-50; and column 6, lines 35-42) *and enabling said authorized user to access said document at said peripheral using said key* (see column 15, lines 45-47 and column 10, line 65 through column 11, line 8). **Gormish et al** suggests using any digital encryption method and any key exchange methods and use of keys as known in the art (see column 6, lines 29-47; column 11, lines 6-7 and column 12, lines 57-59) but does not explicitly disclose encoded the key. **Smith et al** in an analogous art teaches a method and apparatus for authenticating ownership of cryptographic keys comprising generated a key, the

Art Unit: 2136

key is hashed and encoded into a bar code; then the encoding key is communicated to the receiver as the encoded key is applied to the transmitted document (see page 2, paragraphs 18-20 and figure 2). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include the features of encoding as disclosed in **Smith et al** to encode the keys of **Gormish et al** as taught by **Smith et al** (see figure 2). One of ordinary skill in the art would have been motivated to do so because it would provide a secure means to communicate key information associated with the sender and the document (see paragraph 15) as well as way to verify the sender of the document as suggested by **Smith et al** (see page 2, paragraphs 17-21).

4. **Claims 7-9** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,692,048 to **Gormish et al** in view of US Patent Publication 2003/0005298 to **Smith et al** as applied to claims 1-6 and further in view of US Patent Publication US 2002/0042880 to **Endoh**.

As per claims 7-9, both references disclose the claimed method of claim 1. None of the references explicitly disclose specifying a maximum or remaining number of times for the document to be accessed or time of access. **Endoh** in an analogous art teaches managing a job using an access ticket in the job management command comprising means for decrypting the access ticket and controlling means for limiting execution of said control command based on the limit information in the access ticket (see paragraph 8). Examples of limiting values of the printing job include permitted number of prints and time of access as of each login, including expiration date, etc. (see paragraph 69 and 95) and remaining number of prints (see paragraph 115), the printing job is further associated with the login time of permission to use (permission to

Art Unit: 2136

access) and in the case where permission to use is not given login is not permitted (see paragraph 125-127). This meets the recitation of wherein the encryption specifies a maximum number of times the encrypted document is to be accessed (see paragraphs 112 and 117), wherein a remaining number of times the document is available for output is indicated (see paragraph 110 and 130-131), and wherein the encryption specifies a time by which the encrypted document is to be accessed (see paragraph 170). (See also page 11, paragraphs 170-175). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method as combined above to use an access ticket indicating of maximum number of times, time of access, remaining time available for output as suggested by **Endoh**. One of ordinary skill in the art would have been motivated to do so to provide access control so that the use of the equipment by each user can be managed as disclosed by **Endoh** (see paragraphs 7 and 224).

Conclusion

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

Art Unit: 2136

however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

5.1 The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. The prior art discloses many of the claimed features for accessing a secure document using encryption (See PTO-Form 892).


5.2 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/C.C./
Carl Colin
Patent Examiner
September 5, 2007

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100


9,14107